NanoTrustedDesc format specification

Type: NanoTrustedDesc

A generic binary format for trusted descriptors (an info trusted by the nano signed by a Ledger key)

Table 1. Table NanoTrustedDesc

pos	size	id	type	description
0	1	type	u1 → DescType	Type of the descriptor
1	1	version	bytes={0x01}	Version, currently fixed to 0x01
2	1	key	u1 → KeyEnum	Signing key identifier, unique to Ledger. The corresponding certificate must be passed to the application before use.
3	...	challenge	Challenge	An optional challenge to prove freshness of the descriptor
???	...	body	#type value: format plugin: PluginBody nft: NftBody name: NameBody	Body of the descriptor, based on type
???	...	sig	Signature	Signature of the descriptor computed over other fields

Enum: DescType

value	id	description
plugin	1	a plugin descriptor, mapping a smartcontract address to a nano plugin
nft	2	an nft collection descriptor, mapping an NFT address to a collection name
name	3	a trusted name descriptor, mapping a blockchain address to a displayable name

Enum: KeyEnum

value	id	description
test	1	test key, do not use in prod
persov2	2	PersoV2 Signing Key 01
plugin_selector_key	3	AWS Plugin Selector Signing Key 01

Type: NftBody

An NFT collection descriptor

Table 2. Table NftBody

pos	size	id	type	description
0	1	len_name	u1	Length of the name field
1	len_name	name	bytes	UTF-8 encoded name of the collection corresponding to the address
???	20	address	bytes	Blockchain smartcontract address associated with this collection
???	8	chain_id	bytes	Blockchain id, as specified in XXX

Type: Challenge

An optional challenge enabling proving freshness of the descriptor

Table 3. Table Challenge

pos	size	id	type	description
0	1	len_challenge	u1	length of the challenge, when no challenge is present use length of 0x00
1	len_challenge	challenge	bytes	challenge as an array of raw bytes

Type: PluginBody

A plugin descriptor

Table 4. Table PluginBody

pos	size	id	type	description
0	1	len_name	u1	Length of the name field
1	len_name	name	bytes	ASCII encoded name of the plugin to use
???	20	address	bytes	Blockchain smartcontract address associated with this plugin

pos	size	id	type	description
???	4	selector	bytes	function selector in the smartcontract associated with this plugin
???	8	chain_id	bytes	Blockchain id, as specified in XXX

Type: Signature

a signature container

Table 5. Table Signature

pos	size	id	type	description
0	1	len_sig	u1	Signature length
1	len_sig	sig	bytes	DER encoded signature. Signature is computed over serialized fields [type , version , key , challenge , body]. Signature key and algorithm is determined by the [key] field and corresponding certificate.

Type: NameBody

A trusted name descriptor

Table 6. Table NameBody

pos	size	id	type	description
0	1	len_name	u1	Length of the name field
1	len_name	name	bytes	UTF-8 encoded truted name associated with this address
???	4	coin_type	bytes	SLIP 44 coin type as in [https://github.com/ensdomains/address-encoder]
???	1	len_address	u1	Length of the address field
???	len_address	address	bytes	Address value for this trusted name